STUDY ON GEOGRAPHIC LOCATION BASED SECURED AUTHENTICATION SYSTEM

Borse Yogeshwari Suklal,[1] Dr. Anil Kumar[2]

[1] *Research Scholar, Computer Science & Engineering, SSSUTMS, Sehore, M.P. India*
[2] *Professor, Computer Science & Engineering, SSSUTMS, Sehore, M.P. India*

ABSTRACT

With the growth of wireless technologies in sectors like the military, aviation, etc, there is a need to determine the authenticity of a genuine user. The location-based authentication is a quite new direction in the information security. The direction gains in importance nowadays due to mobile devices coming to wireless network environment. Authentication is accepting proof of identity given by a credible person who has evidence on the said identity or on the originator and the object under assessment as his artifact respectively. Traditional authentication technique generally requires an id and password to verify the identity of user. By nature, user is looking for a password that is easy to remember and secured from any attack. However, remembering many complicated passwords, especially when user has different accounts, is not an easy task. Earlier two factor authentication technique is common in use. In the two factor authentication individual can be identified by his user name and password. If username and password is matched then process of authentication is done and user can access the data. But in this technique anyone can hack password and access information.

Keyword: - *Wireless Technologies1, Authentication2, Username and password 3, Computer Networks4.*

1. NETWORK SECURITY

Networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. Networks are comprised of “nodes”, which are “client” terminals (individual user Personal Computers), and one or more “servers” and/or “host” computers.

They are linked by communication systems, some of which might be private, such as within a company and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications.

Today, most companies' host computers can be accessed by their employees whether in their office over a private communications network or from their homes or hotel rooms, while on the road through normal telephone lines. Network security involves all activities that organizations, enterprises and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them [1-4].

2. LITTERATUE SURVEY

Renaud et al. [30] make comparison how users responded to traditional text challenge questions and picture-based challenges for both name-based and location-based questions. Where the location-based questions were often answered incorrectly in both cases, due to the fact that users were needed to enter a text city and country name, which lead them to a incorrect inputs by users. In GeoPass, users may input text in the search bar, but if the text is not proper then they will receive instant feedback as the map they are shown would be different than what they intended to search for. And also, when users give's input text into the search bar, they are presented with a drop-down list from which they choose their intended search term [31-41]. While entering a location password in GeoPass is more time consuming than typing a text name, its design aids the usability of correctly entering exact locations. Authentication through a digital map can be seen as a type of graphical password.

Denning and Macdorman [42] were among the first authors to perform research studies about location-based authentication and to highlight its importance for improving network security. In a virtual environment where physical borders are blurred, location determination during authentication can be helpful in many scenarios e.g. remote access to critical systems, authenticating financial transactions, enforcing export controls on software and so on. They describe a technology by the International Series Research in USA, called CyberLocator, which is used to achieve location-based authentication by using what is called a location signature. A client that wants to access a protected resource is challenged to provide a location signature, which is then verified by the server. The server does this by also computing its own location and comparing it to the one provided by the client.

Since the location signature is unique for each location at any given time, this information cannot be spoofed or replayed later. However, in order to achieve this, CyberLocator needs its clients to possess a special kind of GPS sensor that is different to the ones that are commercially available [43-56].

YounSun et al. [57] propose a location–aware access control mechanism (LAAC) based on a WLAN infrastructure of wireless access points and wireless mobile devices, such as PDAs and wireless laptops. Access is granted to a device located inside a region formed by overlapping coverage of multiple access points. Each access point periodically broadcasts a random nonce which is captured and used by the device to generate a location key.

Devices outside the range of the access points won't be able to receive these random nonces and consequently won't be able to derive valid location IDs. In this way access is granted only within specific locations.

Bao [58] proposes similar mechanism using wireless access points. His system is known as LENA (Location Enforced Network Access). LENA has two schemes, one known as LENA-SK (LENA using Security Keys) uses

Diffie-Helman key exchange protocol to authenticate user location, authorize network access, and distribute a key for data encryption. The other scheme, LENA-PAP (LENA using Personal AP Protocol) uses mobility management protocol to ensure authenticity of location claims. These mechanisms are designed specifically for controlling access to wireless networks.

Jansen and Kolorev [59] designed a location–based authentication mechanism that involves policy beacons and mobile devices. These policy beacons broadcast and communicate location data to mobile devices using Bluetooth. Mobile devices determine their proximity to beacons and calculate their location relative to them. Based on this location certain functionalities in the mobile devices are enabled or disabled accordingly. Policy beacons establish a perimeter with a distinct organization policy. Devices within this perimeter inherit this policy. Their setup, however, focuses only on controlling the use of mobile devices, especially in an environment such as in an organization and it requires a significant costly infrastructure setup and synchronization of policy beacons [60-65].

Takamizawa and Kaijiri [66-68] proposed and designed an authentication method using location information obtained from mobile telephones that is suitable in web-based education applications. A student who wants to login into the web-based application, in addition to using username and passwords, has also to provide his/her location through a mobile telephone in order to prove the authenticity. In their method, location from a mobile phone is determined using GPS. For that, mobile phone must be equipped with a GPS receiver and a clear view of the sky is needed for the process to work. QR codes are also used for web applications to prompt the mobile phone for the location. The user has to scan the code from the screen using his/her mobile phone and therefore a phone needs a camera. In addition, the authors did not pay attention to security threats and vulnerabilities for their location–based authentication method and as such the mechanism may be susceptible to trivial attacks. For example, the location could be easily spoofed or modified [69-70]. Ardagna et al. [71] analyzed how location information can be used to strengthen access control mechanisms by adding features for defining and enforcing location–based policies. They proposed design of a Location–based Access Control (LBAC) architecture and provided an extension to the XAMCL policy language (introduced by the Open Geospatial Consortium – OGC) for defining and describing geographic location coordinates. This extension is known as GEOXAMCL. They showed examples of how this can be used to express access control rules that can be used in a typical application.

3. CONCLUSION

Some of the existing solutions have been focused on designing and constructing general conceptual security models for these kinds of mechanisms. Some have demonstrated and justified the use of location in improving existing security mechanisms. Despite the security features that they offer, most of these solutions however have suffered from problems such as practicality, usability, reliability and cost. In addition since the location signature depends on GPS, the mechanism suffers a lot of reliability issues especially indoors or in places where there is no clear view of the sky. Others have proposed protocols, which however apply only to specific scenarios or require specific devices. A general and flexible approach that can be applied in different situations is still lacking

REFERENCES

1. Mathur, Surbhi, et al. "Methodology for partial fingerprint enrollment and authentication on mobile devices." Biometrics (ICB), 2016 International Conference on. IEEE, 2016.

2. Khan, Muhammad Khurram, Jiashu Zhang, and Xiaomin Wang. "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices." Chaos, Solitons & Fractals 35.3 (2008): 519-524.

3. Xi, Kai, et al. "A fingerprint based biocryptographic security protocol designed for client/server authentication in mobile computing environment."Security and Communication Networks 4.5 (2011): 487499.

4. Shila, Devu Manikantan, et al. "A multi-faceted approach to user authentication for mobile devices—Using human movement, usage, and location patterns." Technologies for Homeland Security (HST), 2016 IEEE Symposium on. IEEE, 2016.

5. Gurary, Jonathan, et al. "Implicit Authentication for Mobile Devices Using Typing Behavior." International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, 2016.

6. Teh, Pin Shen, et al. "TDAS: a touch dynamics based multi-factor authentication solution for mobile devices." International Journal of Pervasive Computing and Communications 12.1 (2016): 127-153

7. Gross, Aurel. "Using Geolocation Authentication and Fraud Detection for Web-Based Systems." Master's Thesis, Athabasca University (2011). Gorde, Swati, et al. "Secure Online Bank Authentication Using Geolocation Based System." Imperial Journal of Interdisciplinary Research 2.6 (2016).

8. Klein, Elliot. "Gps location authentication method for mobile voting." U.S. Patent Application No. 12/635,847.

9. Frank Diekmann, "Survey: Mobile Bankers Double Over Last Year." Credit Union Journal, vol. 15, no. 18, pp. 19-19, May 2011.

10. G. Sun, J. Chen, W. Guo, and K.J.R. Liu, "Signal processing techniques in network aided positioning: a survey of state-of-the-art positioning designs." IEEE Signal Processing Magazine, vol. 22, no. 4, pp. 12-23, 2005.

11. U.S. Government,“Official U.S. Government information about the Global Positioning System (GPS) and related topics.”Internet: www.gps.gov, Apr. 20, 2012 [May 15, 2012].

12. Paul A. Zandbergen, "Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning." Transactions in GIS, vol. 13, no. s1, pp. 5-25, 2009.

13. Skyhook, “Skyhook.”Internet: www.skyhookwireless.com, [May 15, 2012].

14. Axel Kuepper. Location-Based Services: Fundamentals and Operation. Wiley Online Library, Oct. 2005.

15. TruePosition, U-TDOA: Enabling New Location-Based Safety and Security Solutions, Oct. 2008.

16. S.Z. Li and A.K. Jain.Encyclopedia of Biometrics. US, Springer US, 2009.

17. D. Denning and P. MacDoran, "Location-Based Authentication: Grounding Cyperspace for Better Security." Computer Fraud and Security Bulletin, Feb. 1996.

18. A.I.G.T. Ferreres, B.R. Alvarez, and A.R. Garnacho, "Guaranteeing the authenticity of location information." IEEE Pervasive Computing, pp. 72-80, 2008.

19. S. Lo, D.S. De Lorenzo, P.K. Enge, D. Akos, and P. Bradley, "Signal authentication-a secure civil gnss for today." inside GNSS, vol. 4, no. 5, pp. 30-39, 2009.

20. G. Becker, S. Lo, D. De Lorenzo, P. Enge, and C. Paar, "Secure Location Verification." Data and Applications Security and Privacy XXIV, 2010, pp. 366-373.

21. Haeberlen et al., "Practical robust localization over large-scale 802.11 wireless networks." in Proceedings of the 10th annual international conference on Mobile computing and networking, ACM, 2004, pp. 70-84.

22. S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs." Proceedings of the 10th workshop on Mobile Computing Systems and Applications, New York, USA, 2009, pp. 3:1--3:6.

23. W. Luo and U. Hengartner, "VeriPlace: a privacy-aware location proof architecture." Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, ACM, 2010, pp. 23-32.

24. Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services." INFOCOM, 2011 Proceedings IEEE, 2011, pp. 1889-1897.

25. V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: applications, challenges and implementations." Proceedings of the 9th workshop on Mobile computing systems and applications, ACM, 2008, pp. 60-64.

26. L. Scott and D.E. Denning, "A location based encryption technique and some of its applications." in ION National Technical Meeting, vol. 2003, 2003, pp. 730-740.

27. Al-Fuqaha and O. Al-Ibrahim, "Geo-encryption protocol for mobile networks," Computer Communications, vol. 30, no. 11-12, pp. 2510-2517, 2007.

28. G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular adhoc networks." IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, MASS'09, 2009, pp. 804-809.

29. G. Yan, J. Lin, D.B. Rawat, and W. Yang, "A Geographic Location-Based Security Mechanism for Intelligent Vehicular Networks." Intelligent Computing and Information Science, pp. 693-698, 2011.

30. W.B. Hsieh and J.S. Leu, "Design of a time and location based One-Time Password authentication scheme." Wireless Communications and Mobile Computing Conference (IWCMC), 7th International, IEEE, 2011, pp. 201-206.

31. H.C. Liao and Y.H. Chao, "A new data encryption algorithm based on the location of mobile users." Information Technology Journal, vol. 7, no. 1, pp. 63-69, 2008.

32. L. Scott and D.E. Denning, "Location Based Encryption & Its Role In Digital Cinema Distribution." Tech. rep. 2003.

33. Ihsan A. Lami, Torben Kuseler, Hisham Al-Assam, and Sabah Jassim, "LocBiometrics: Mobile phone based multifactor biometric authentication with time and location assurance," Proc. 18th Telecommunications Forum, IEEE Telfor, Nov. 2010.

34. Torben Kuseler, Hisham Al-Assam, Sabah Jassim, and Ihsan A. Lami, "Privacy preserving, real-time and location secured biometrics for mCommerce authentication," SPIE Mobile Multimedia/Image Processing, Security, and Applications 2011, vol. 8063, Apr. 2011.

35. Giordano, M. Chan, H. Habal, “A Novel Location-Based Service and Architecture”, IEEE 1995, pp. 853–857.

36. A.P. Sistla, O. Wolfson, S. Chamberlain, and S. Dao, “Modeling and Querying Moving Objects”, Proc. 13tg Int’l Conf. Data Eng. (ICDE ’97), 1997.

37. Andrew S. Tannenbaum, “Modern Operating Systems”, Prentice Hall, 1992.

38. Andy Marhs, Michael May, Markuu Saarelainen, “Pharos: Coupling GSM & GPS-TALK technologies to provide orientation, navigation and location-based services for the blind”, IEEE 2000, pp. 38–43.

39. Arnon Rosenthal, Edward Sciore, “Extending SQL’s Grant Operation to Limit Privileges”, IFIP Workshop on Database Security, Amsterdam, August 2000.

40. Chadha, Kanwar, “The Global Positioning System: Challenges in Bringing GPS to Mainstream Consumers”, ISSCC98, February 5, 1998.

41. Christian S. Jensen, Anders Friis-Christensen, Torben Bach Pedersen et.al., “Location-based services: A database perspective”, ScanGIS 2001: pp. 59-68.

42. Christopher Rose, Roy Yates, “Location Uncertainty in Mobile Networks: A Theoretical Framework”, IEEE Communication Magazine, February 1997, pp. 94–101.

43. Do van Thanh, Jan Audestad, “Making Mobility Transparent to the Application”, IEEE 1996, pp. 1825–1829.

44. Dorothy E. Denning, Peter F. MacDoran, “Location-based Authentication: Grounding Cyberspace for Better Security, Internet besieged: countering cyberspace scofflaws”, Addison Wesley 1998, pp. 167–174.

45. Dragan H. Stojanovic, Slobodanka J. Djordjevic-Kajan, “Developing Location-based Services from a GIS Perspective”, IEEE 2001, pp. 459–462.
46. Evaggelia Pitoura, George Samaras, “Locating Objects in Mobile Computing”, IEEE 2001, pp. 571–592.

47. George Kollios, Dimitrios Gunopulos and Vassilis J. Tsotras, “On indexing mobile objects”, Proceedings of the Eighteenth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems May 31 - June 3, 1999, Philadelphia, PA USA, pp. 261272.

48. Guanling Chen, David Klotz, “A Survey of Context-Aware Mobile Computing Research”, Dartmouth Computer Science Technical Report TR2000-381, 2000.

49. Henning Maaß, “Location-aware Mobile Applications Based on Directory Services”, Proceedings of the third annual ACM/IEEE international conference on Mobile computing and networking, 1997, pp. 23–33.

50. Hui Luo, N. K. Shankaranarayanan, “A Conditional E-Coupon Service For Location-Aware Mobile Commerce, Internet besieged: countering cyberspace scofflaws”, Addison Wesley 1998, pp. 587–601.

51. IETF Geographic Location/Privacy (geopriv) Working Group, http://www.ietf.org/html.charters/geopriv-charter.html
52. J. Mäkelä, M. Ylianttila, K. Pahlavan, “Handoff Descision in Multi-Service Networks”, IEEE 2000, pp. 655–659.

53. James M. Zagami, Steen A. Parl, Julian J. Bussgang, Karen Devereaux Melillo, “Providing Universal Location Services Using a Wireless E911 Location Network”, IEEE Communications Magazine, April 1998, pp. 66–71.

54. Java Location Services, http://www.jlocationservices.com/

55. Kou-Chen Wu, Lir-Fang Sun, “A Self-served Mobile Location Query Service”, IEEE 2001, pp. 126–129.

56. Local.info product from SignalSoft Corporation; product description: http://www.signalsoftcorp.com/newsroom/media/datasheets/Slick - li new final.pdf.

57. Location Interoperability Forum (LIF), http://www.locationforum.org/

58. Michael F. Worboys, “GIS: A Computing Perspective”, Taylor & Francis, 1995. Open Location Initiative (OpenLS Initiative), http://www.openls.org/

59. OpenGIS, “OpenGIS Simple Features Specification For SQL”, Open GIS Consortium, Inc., http://www.opengis.org/techno/specs/99-049.pdf, May 1999.

60. Ouri Wolfson, Prasad Sistla, Bo Xu, Jutai Zhou and Sam Chamberlain, “DOMINO: databases for Moving Objects tracking”, Proceedings of the 1999 International Conference on Management of Data, 1999, pp. 547–549.

61. P. Bahland and V.N. Padmanabhan, “RADAR: An In-Building RF-Based User Location and Tracking System”, Proc. IEEE Infocom 2000, IEEE Press, Piscataway, N.J., 2000, pp. 775784.

62. Pitoura, E. Samaras, G., „Locating Objects in Mobile Computing“, IEEE Transactions on Knowledge and Data Engineering, Volume 13 Issue 4, July-Aug. 2001, pp. 571–592.

63. Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P/.

64. Raghu Ramakrishnan, Johannes Gehrke, “Database Management Systems”, Second Edition, McGraw Hill, 2000.

65. Rui José, Adriano Moreira, Filipe Meneses, Geoff Coulson, “An Open Architecture for Developing Mobile Location-Based Applications over the Internet”, IEEE 2001, pp. 500 – 505.
66. S. Shekhar, D. Lui, “CCAM: A Connectivity-Clustered Access Method for Networks and Network Computations”, IEEE Transactions on Knowledge and Data Engineering, Volume 9 Issue 1, Jan-Feb 1997, pp. 102-119.

67. S. Shekhar, S. Chawla, “A Tour of Spatial Databases (Draft)”, August 2001. Sandrine Mérigeault, Mickael Batarière, Jean Noel Patillon, “Data Fusion Based on Neural Network for the Mobile Subscriber Location”, IEEE 2000, pp. 536–540.

68. Sophie Cluet, Olga Kapitskaia, Divesh Srivastava, “Using LDAP Directory Caches”, ACM 1999, pp. 273–284.

69. Tomasz Imielinski, Julio C. Navas, “GPS-Based Geopgraphic Addressing, Routing, and Resource Discovery”, Comm. of the ACM, April 1999, Vol 42. No. 4, pp. 86–92.

70. Zagami, J.M., Parl, S.A., Bussgang, J.J., Melillo, K.D., “Providing universal location services using a wireless E911 location network”, IEEE Communications Magazine, Volume: 36 Issue: 4, April 1998, pp. 66–7.

71. Zygmunt J. Haas, “Location-Independent Access in Mobile Systems”, IEEE 1996, pp. 255–259.